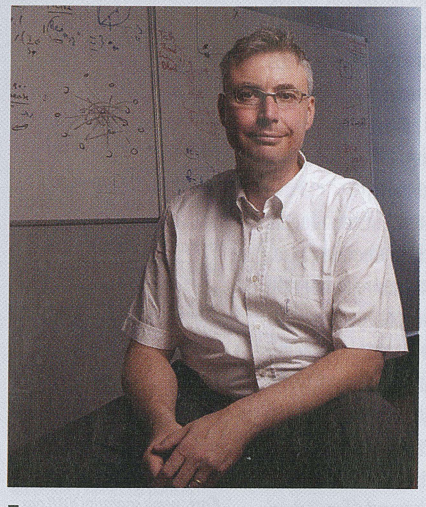
Informatique et société : Sécuriser les téléphones portables : entretien avec Olivier Festor et Abdelkader Lahmadi

Festor Olivier, Abdelkader Lahmadi

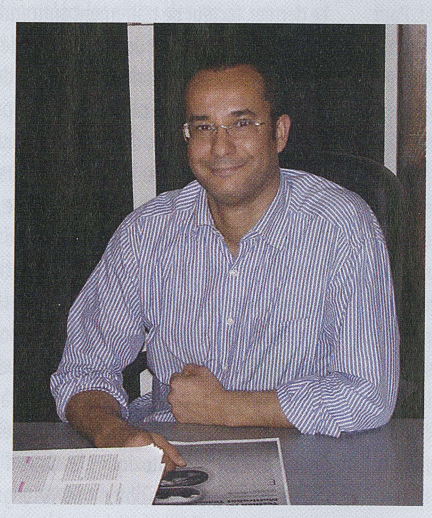
Sécuriser les téléphones portables

ENTRETIEN AVEC OLIVIER FESTOR ET ABDELKADER LAHMADI

Peu nombreux furent ceux à avoir anticipé l'ampleur de la délinquance que nous connaissons aujourd'hui sur l'Internet. Dans les prochaines années, ce sont nos mobiles qui pourraient être de plus en plus visés.



© INRIA / KAKSONEN



© D.R.

Olivier Festor (à gauche), directeur de recherche Inria, est responsable scientifique de l'équipe-projet Madynes (Inria Nancy - Grand Est). Abdelkader Lahmadi (à droite), maître de conférences à l'Institut national polytechnique de Lorraine, est membre de l'équipe-projet Madynes.

Quels sont les problèmes de sécurité identifiés à ce jour sur les mobiles ?

Olivier Festor : Désormais, le téléphone mobile est devenu un ordinateur comme un autre, connecté en permanence à Internet et avec des capacités de calcul et des applications qui le rendent tout aussi vulnérable. Or il faut savoir qu'un ordinateur subit en moyenne 200 à 300 attaques par jour : la première attaque sur une machine équipée d'un système Windows intervient en moyenne 30 secondes après son branchement sur le réseau ! En ce qui concerne les téléphones, les attaques sont beaucoup plus diversifiées, le vecteur le plus problématique étant aujourd'hui le SPam over Internet Telephony, ou SPIT, très intrusif : il s'agit, soit de SMS, soit d'appels téléphoniques, générés par des robots. Il faut compter en plus avec les attaques dont sont classiquement victimes les machines connectées à Internet (vers, virus, en pleine expansion sur les mobiles). Ces dangers se trouvent amplifiés par trois facteurs : la confiance que les utilisateurs font *a priori* à leur téléphone, le fait que le coût de ces attaques soit quasi-nul pour les attaquants, et enfin la diffusion extrêmement rapide des téléphones portables.

Le réseau de téléphonie mobile se trouve donc fragilisé ?

Abdelkader Lahmadi : Le réseau GSM* était très bien sécurisé. Il l'est nettement moins depuis que des passerelles ont été établies avec le monde de l'internet et que les terminaux opèrent sur plusieurs réseaux en parallèle. Cela n'avait pas été anticipé, ni dans la mise en place des services ni dans la définition des normes.

D'où la nécessité de développer des logiciels pour sécuriser la téléphonie mobile et la téléphonie sur Internet ?

O. F. : Deux niveaux sont à considérer : le niveau « terminal » et le niveau « opérateur ». En ce qui concerne le niveau « opérateur », nous avons travaillé sur un pare-feu de signalisation, Secsip, qui s'appuie sur des techniques d'inspection de messages. Cet outil permet à l'opérateur de décrire les *patterns* de trafic qu'il souhaite bloquer. Il s'agit essentiellement de bloquer des attaques de signalisation, à savoir des messages envoyés aux téléphones pour leur faire exécuter des actions non souhaitées.

Et pour protéger les terminaux ?

A. L. : Nous nous sommes penchés sur un aspect bien particulier : le blocage des SMS (voire des appels téléphoniques) non sollicités. C'est le but du logiciel Hinky, qui tourne sur le système d'exploitation Android*. Hinky est capable d'identifier les SMS malveillants à partir d'une base de connaissances, celle-ci étant complétée en permanence de manière communautaire : chacun peut la compléter au fur et à mesure (après divers niveaux de vérification bien sûr) avec les nouveaux messages malveillants détectés. Actuellement, Hinky est l'un des principaux logiciels de ce type dans le monde à être ainsi directement téléchargeable sur le téléphone.

Quelles sont les étapes suivantes ?

O. F. : En ce qui concerne le pare-feu (SecSIP), nous travaillons sur l'automatisation de la génération de règles : l'idée est de générer automatiquement la règle qui permettra de bloquer une nouvelle attaque. Quant à l'aspect antispam (Hinky), le sujet n'en est qu'à ses débuts. Pour l'instant, nous nous efforçons surtout de collecter le maximum d'informations avant de nous associer à d'autres équipes plus spécialisées dans la classification et la fouille de données. L'enjeu est d'importance : il est prévu que d'ici à cinq ans, le phénomène spam pourrait avoir la même ampleur sur le téléphone que sur nos ordinateurs actuels.

Propos recueillis par Dominique Chouchan

* Le *Global System for Mobile Communications*, ou GSM, est la norme de téléphonie mobile la plus utilisée dans le monde.

* Android est un système d'exploitation partiellement en *open source* pour téléphones intelligents (*smartphones*), terminaux mobiles…